DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy #16: Information Assurance & Vulnerability Assessment

1. References:

a. AR 25-1, Army Knowledge Management and Information Technology, 15 July 2005.

b. AR 25-2, Information Assurance, 14 November 2003

c. HQDA CIO/G6 Information Assurance Vulnerability Management Program, Army Information Assurance web page, https://informationassurance.us.army.mil

d. Army Policy for the Implementation of the Information Assurance Vulnerability (IAVA) Process, https://www.acert.1stiocmd.army.mil/policy/Army_IAVA_Policy.txt

2. Purpose: The Army Information Assurance Vulnerability Management Program promulgates messages to all system administrators alerting them of vulnerabilities found on AIS devices and software. The messages titled, *Information Assurance Vulnerability Alerts (IAVA),* describe the devices/software affected, prescribes corrective actions to correct or mitigate the vulnerability, and establish suspense for completion of the corrective actions. This policy describes the method of IAVA program enforcement within the 4ID area of responsibility. IAVA messages are promulgated by a list server and posted on Army Knowledge Online. Every Information Assurance Security Officer (IASO), Systems Administrator (SA), and IA Manager (IAM) must subscribe to the IAVA list server.

3. Applicability: This policy is applicable to all United States military personnel, and to civilians serving with, employed by, or accompanying the Armed Forces of the United States, while assigned to the 4th Infantry Division or while present in the 4th Infantry Division's AOR who plan, deploy, configure, operate, and maintain Automated Information Systems (AIS) directly or indirectly attached to 4ID networks.

4. Policy: This policy provides direction for 4ID personnel and tenants as it relates to Information Assurance & Vulnerability Assessment (IAVA) compliance.

a. The Division Information Assurance (IA) Cell or supporting IA Cell will send out a list of non Information Assurance & Vulnerability Assessment (IAVA) compliant computers and Regional Emergency Response Team (RCERT) tickets within the 4ID network.

b. Upon receipt of the non IAVA compliant computers, units will have 72 hours to correct their discrepancies.

c. After 72 hours, if a unit is still non IAVA compliant, the machine and port will be disabled. The port and machine will be re-enabled until the unit reports compliance.

5. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding